

DNS - BIND

Instalar e Configurar, Primário, Secundário e Reverse

1. Instalar Serviço DNS

```
yum install bind9 bind9-utils
```

2. Configurar Serviço de DNS (bind)

Antes de iniciar amos colocar o BIND no modo IPv4, já que nossa rede privada usa exclusivamente o IPv4. Para tal:

A. Editar o ficheiro: /etc/default/named e definir no final do ficheiro

```
#
# run resolvconf?
RESOLVCONF=no

# startup options for the server
#OPTIONS="-u bind"
OPTIONS="-u bind -4"
```

B. Fazer restart do serviço

```
systemctl restart bind9.service
```

C. Editar o ficheiro: /etc/bind/named.conf.options e definir ACLs e o endereço IP do servidor de DNS

```
acl trusted {192.168.57.0/24; 172.20.104.0/24; <IP_ou_ENDEREÇO_REDE;>;};

options {
    directory "/var/cache/bind";

    recursion yes;                                # enables recursive queries
    allow-recursion {trusted;};
    listen-on { <ip-servidor-dns>; }; #ns1 private IP address
    allow-transfer { none; };                    #disable zone-transfers by default

    forwarders {
        172.20.6.100;
        8.8.8.8;
    };
    empty-zones-enable no;
};
```

Obs: acl (access-control-list) permitem definir listas de IPs ou redes que podem depois ser usadas para permitir ou negar pedidos ao servidor de DNS ou a domínios em específico.

D. (Re)Iniciar o serviço: systemctl restart bind9.service

E. Definir serviço para arrancar automaticamente: systemctl enable bind9.service

F. Verificar estado do serviço: systemctl status bind9.service

3. DNS Zonas (domínios Internet) – Primário, Secundário

Sendo o DNS um serviço central ao funcionamento das redes de comunicação é vital a existência de mecanismos que permitam o funcionamento do serviço com elevada disponibilidade. A configuração do DNS em dois servidores alternativos, designando-se um por primário (*master*) e o outro por secundário (*slave*) é usual e dá maior garantias sobre o funcionamento do serviço.

A configuração primário/secundário é bastante simples. Vejamos os ficheiros de configuração em ambos os servidores.

[Primário]

- A. Editar ficheiro `/etc/bind/named.conf.local` e criar a zona indicando o ficheiro de hosts e o tipo de servidor para a zona (master/slave)

```
zone "<nome_da_zona (exemplo empresaA.com)>" {
    type master;
    file "/etc/bind/zones/<ficheiro_hosts (exemplo: empresaA.com.db)>";
    allow-query {trusted;};
    allow-transfer { <endereço IP do servidor secundário;> };
};
```

- B. Criar o ficheiro “file” indicado na zone (ex: `/etc/bind/zones/empresaA.com.db`) com o conteúdo

```
$TTL 1D
empresaA.com.      IN      SOA      ns1.empresaA.com.      . (
                    2021120701    ;Serial
                    28800         ;Refresh
                    3600          ;Retry
                    604800        ;Expire
                    38400         ;Minimum
                    )
                    IN      NS       ns1.empresaA.com.
                    IN      NS       ns2.empresaA.com.
                    IN      MX       10 smtp.empresaA.com.

ns1      IN      A       <ip-servidor-dns_ns1>
ns2      IN      A       <ip-servidor-dns_ns2>
smtp     IN      A       <ip_servidor_smtp>
pop3     IN      CNAME   smtp
www      IN      A       <ip_servidor_http>
```

Obs: **Fazer o reload do serviço para assumir alterações:** `systemctl reload named.service`

- C. Indicar no ficheiro `/etc/resolv.conf` das máquinas qual o servidor de DNS a contactar

```
nameserver <endereço_IP_servidor_NS1>
nameserver <endereço_IP_servidor_NS2>
```

[Secundário]

- A. Editar ficheiro : `/etc/bind/named.conf.options` `/etc/bind/named.conf.options` configurar o servidor secundário (à semelhança do que foi feito no primário)
- B. Criar a zona `/etc/bind/named.conf.local` indicando ficheiro de hosts e o tipo de servidor para a zona (master/slave)

```
zone "<nome_da_zona (exemplo empresaA.com)>" {
    type slave;
    file "<ficheiro_hosts (ex: empresaA.com.db)>";
    allow-query {internals;};
    masters { <endereço IP do servidor primário;> };
};
```

Obs1: O ficheiro indicado em **file** é criado e atualizado automaticamente a partir do primário. O ficheiro será transferido para o diretório `/var/cache/bind/`

Obs2: As alterações no DNS devem ser feitas sempre no primário. Deve ser igualmente atualizado o valor do “Serial” e feito o *reload* do serviço.

Obs3: Para fazer o reload do serviço: `systemctl reload named.service`

- C. Indicar no ficheiro `/etc/resolv.conf` das máquinas qual o servidor de DNS a contactar

```
nameserver <endereço_IP_servidor_NS1>
nameserver <endereço_IP_servidor_NS2>
```

4. DNS Zonas (domínios Internet) – Reverse Address

Tipicamente o DNS é usado para dado um determinado nome e domínio descobrir qual é o IP associado. Existem, no entanto, situações em que é necessário fazer/conhecer o contrário, isto é, dado um determinado IP descobrir o nome associado. Ao longo dos próximos exemplos será mostrada uma configuração do DNS reverse address.

- A. Editar ficheiro `/etc/bind/named.conf.local` e criar a zona indicando do tipo reverse address (`in-addr.arpa`)

```
zone "in-addr.arpa" {
    type master;
    file "/etc/bind/zones/reverse.db";
    allow-transfer { <endereço IP do servidor secundário;> };
};
```

- B. Criar o ficheiro “file” indicado na zone (ex: `/etc/bind/zones/reverse.db`) com o conteúdo

```
$TTL 86400
@      IN      SOA      ns1.empresaA.com.  root.ns1.empresaA.com. (
                        2020120201      ;Serial
                        28800             ;Refresh
                        3600              ;Retry
```

```
        604800      ;Expire
        38400      ;Minimum
    )
    IN      NS      ns1.empresaa.com.

5.10.10.10  IN      PTR    ns1.empresaa.com.
20.5.168.192 IN     PTR    www.qq-coisa.com.
```